



AR
JPW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE


Assignee's Docket No.: 8490.00)
)
Group Art Unit: 2137)
)
Serial No.: 09/651,979)
)
Examiner: Michael Pyzocha)
)
Filing Date: August 31, 2000)
)
Title: Portable Terminal)
)
)

APPEAL BRIEF
A Summary of Argument Begins on Page 14

The fee for this Brief may be billed to Deposit Account
14 - 0225, NCR Corporation.

CERTIFICATE OF MAILING

I certify that this document is addressed to Mail Stop AF, Commissioner of Patents, PO Box 1450, Alexandria, VA 22313-1450, and will be deposited with the U.S. Postal Service, first class postage prepaid, on January 23, 2006.


Gregory A. Welte

1. REAL PARTY IN INTEREST

NCR Corporation.

2. RELATED APPEALS AND INTERFERENCES

None.

3. STATUS OF CLAIMS

Claims 21 - 38 are pending, rejected, and appealed.

4. STATUS OF AMENDMENTS

No Amendments-After-Final have been submitted.

BEST AVAILABLE COPY

01/27/2006 WARDDELRI 00000029 09651979

01 FC:1402 500.00 DA

5. SUMMARY OF CLAIMED SUBJECT MATTER

The Invention

Sketch 1, below, illustrates standard conventions which will be used in this explanation. The top of the Sketch illustrates an encryption operation. PLAIN TEXT is encrypted into CYPHER TEXT using a key K1.

An example of "plain text" would be the phrase

seafood buffet.

This phrase may be encrypted into the cypher text

kbsthoeiwpolsb.

The "i" in the cypher text represents the space character in the plain text (between "d" at the end of "seafood" and the following "b").

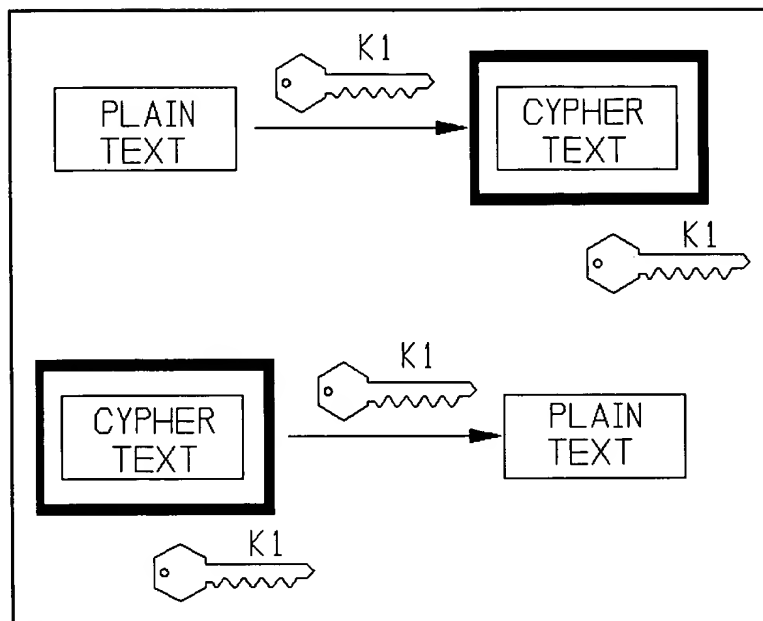
In Sketch 1, the bold box around the CYPHER TEXT represents a lockbox, and the key at the lower right corner of the bold lockbox indicates the key needed to de-crypt the CYPHER TEXT, that is, to "unlock" the lockbox and release the PLAIN TEXT from the lockbox.

The bottom of the Sketch indicates the converse operation. The encrypted CYPHER TEXT is de-crypted using key K1.

Of course, the system can be arranged so that a different key K2 (not shown), as opposed to K1, is needed to perform the de-

09/651,979
Art Unit 2137
Docket No. 8490

ryption.



Sketch 1

Sketch 2 illustrates processes undertaken by the PDA, Personal Digital Assistant (a portable computer), of the invention. (Specification, page 3, line 1; page 6, lines 17, 18; page 8, lines 17, 18. PDA is shown in Figure 4, item 10.)

First, a SEED is created. (Page 8, line 24.)

(In general, a seed is a starting point, or input, for an algorithm which produces a key. Different seeds are used at different times, to produce different keys. An ideal key is a random number, produced by a random number generator. However, as this Brief will explain, it is impossible to produce a truly random number using a digital computer. Nevertheless, digital computers are used to produce keys. Even though these keys are not perfectly random, they are still useful.)

This SEED is derived from data within the memory of the PDA. This data could include the current date, and other data which changes as time progresses. (Page 8, line 25 - page 9, line 2.) In the Sketch, the rectangles represent the data within the memory of the PDA.

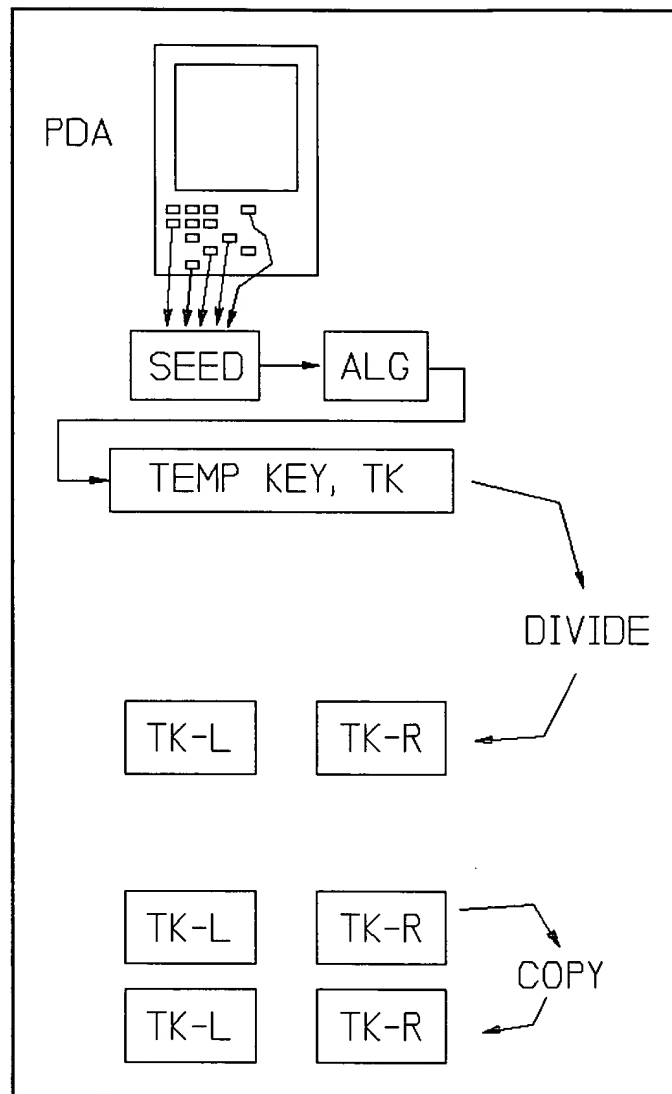
Significantly, this data is not protected: any user of the PDA can gain access to the data. (Page 2, lines 13 - 19. See also page 1, lines 11 - 16; , 27, 28; page 5, lines 13 - 15; page 8, lines 27, 28.)

Next, an algorithm ALG in the Sketch creates a temporary key, TEMP KEY, or TK. Then TK is divided into two halves, left and

09/651,979
Art Unit 2137
Docket No. 8490

right, as shown. (Specification, page 8, line 23 - page 9, line 5. The Specification calls TK a "hash value.")

Finally, the two halves are both copied (conceptually), producing two TK-L's (L: Left) and two TK-R's (R: Right). (Specification, page 9, lines 3 - 7.)



Sketch 2

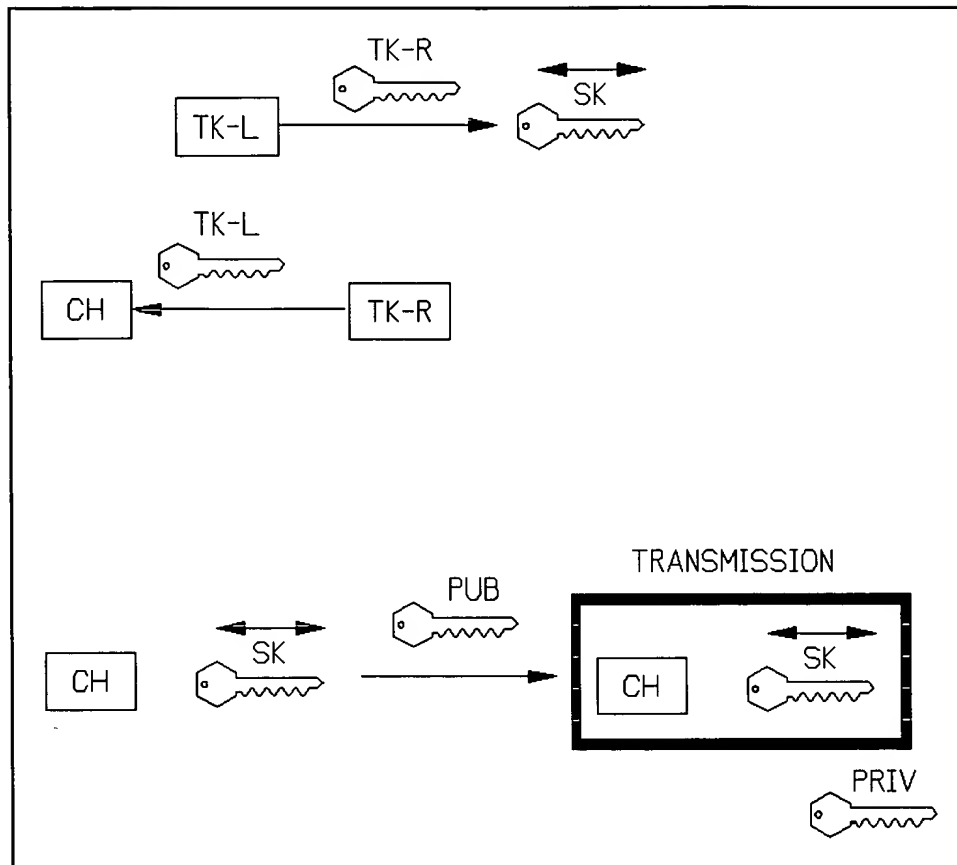
Sketch 3 illustrates further processing within the PDA. TK-R is used as a key to produce a session key SK from TK-L. (In general, a session key is a key which is used for a single "session," and then discarded.) The double arrow indicates that SK is symmetric, meaning that it can both encrypt and de-crypt data. TK-L is used to encrypt TK-R, to produce a challenge CH. (Specification, page 9, lines 6 - 14.)

(In general, a "challenge" is like a password-of-the-day for a clubhouse. You challenge people attempting to enter the clubhouse, by asking for the current password. But the password will be different tomorrow.)

At the bottom of the Sketch, both the newly created CH and SK are encrypted using the public key PUB stored in the PDA. (Specification, page 9, lines 15, 16.) This produces what the Specification calls the TRANSMISSION. (Page 9, line 18.) Note that a private key PRIV is needed to de-crypt the TRANSMISSION. (Specification, page 9, line 20.)

The public key PUB cannot be used for de-cryption, of course, because it is publicly available. If it could be used for the DE-cryption, then the ENcryption would be pointless. Anybody could defeat the encryption by obtaining the publicly available public key.

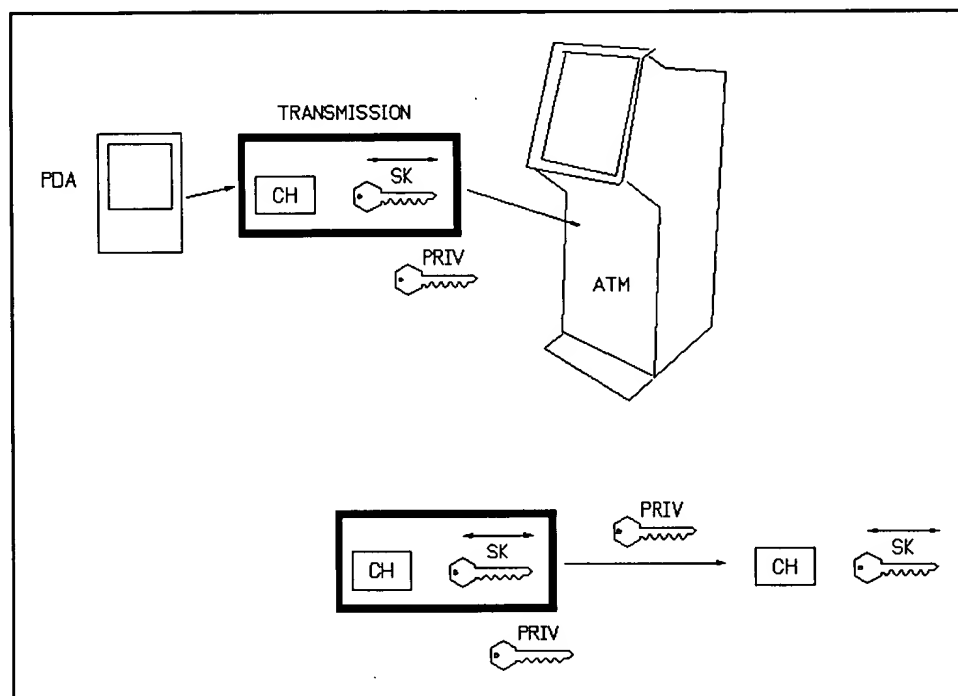
09/651,979
Art Unit 2137
Docket No. 8490



Sketch 3

09/651,979
Art Unit 2137
Docket No. 8490

Sketch 4, top, indicates that the PDA transmits the TRANSMISSION to a terminal, such as an ATM. (Page 9, lines 17, 18.) Sketch 4, bottom, indicates that the ATM de-crypts the TRANSMISSION, using its private key PRIV, to recover the challenge CH and the session key SK. (Specification, page 9, lines 18 - 20.)

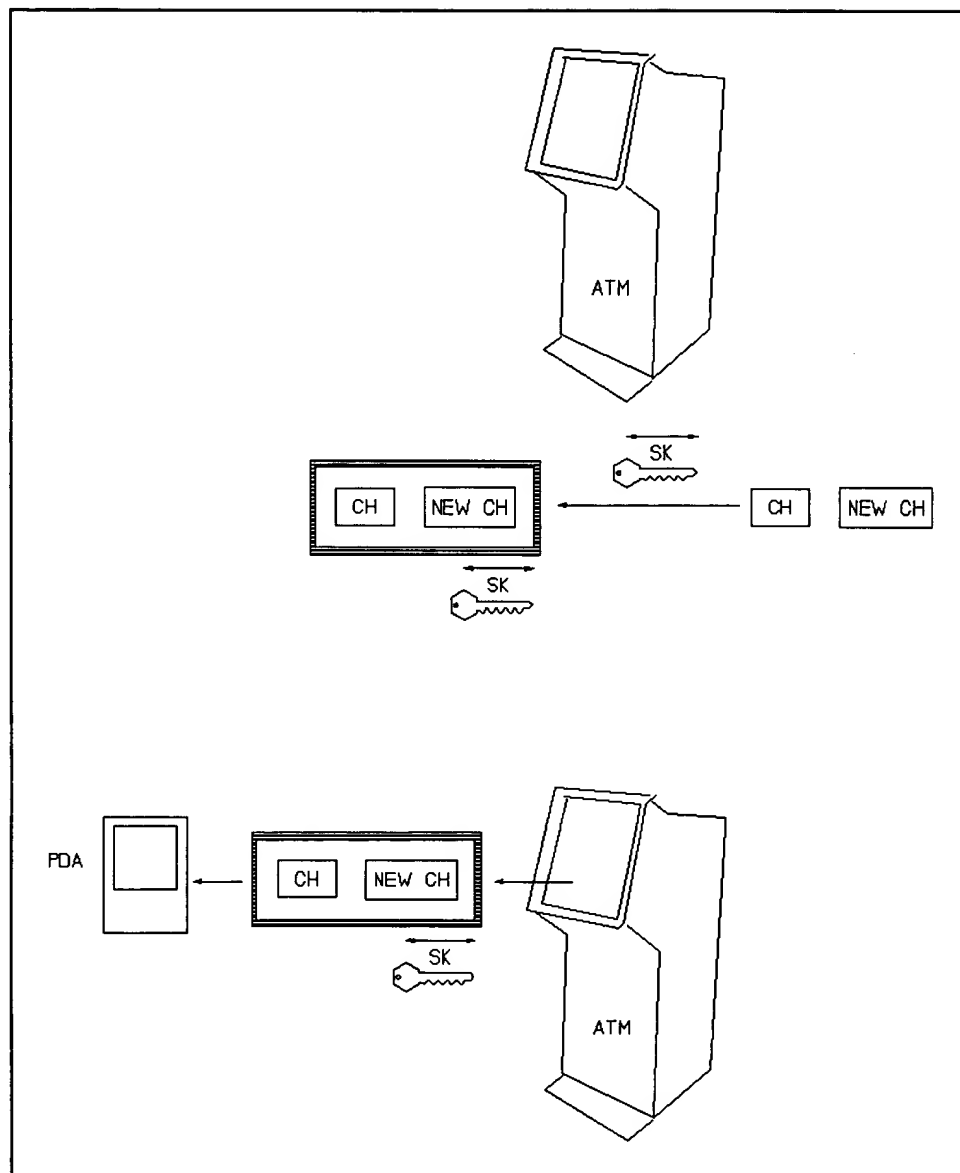


Sketch 4

09/651,979
Art Unit 2137
Docket No. 8490

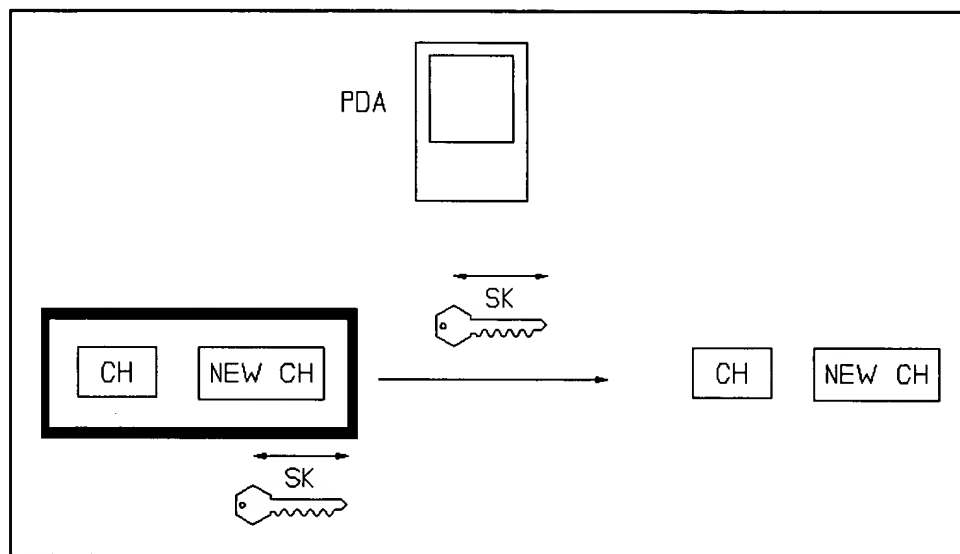
The ATM generates a new challenge NEW CH, based on the challenge CH received. (Specification, page 9, lines 21, 22.) Sketch 5, top, indicates that the ATM encrypts those elements, using the session key SK just received. Sketch 5, bottom, indicates that this encrypted data is transmitted to the PDA. (Specification, page 9, lines 22, 23.)

09/651,979
Art Unit 2137
Docket No. 8490



Sketch 5

Sketch 6 indicates that the PDA de-crypts the data, using the session key SK (created in Sketch 3, top), to recover the challenge CH and the new challenge NEW CH. The PDA can verify whether the ATM is a true ATM through the new challenge NEW CH. If the ATM is an imposter, the PDA can terminate the transaction.



Sketch 6

Identification of "Means"

As required by 37 CFR 41.37(c)(1)(v), Appellant identifies the subject matter supporting the "means" in the claims as follows. Other support is possible.

Claims 30(b) and 32(c) - Figure 2, item 28, and Specification, page 7, line 14 et seq.

Claim 33(a) - Figure 2, item 30, Specification, page 7, lines

09/651,979
Art Unit 2137
Docket No. 8490

3 - 6.

Claim 33(b) - Figure 2, item 34. Specification, page 8, line 25.

Claim 33(c) - Specification, page 8, line 23 et seq.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether the rejection of claims 21 - 38 under 35 USC § 103 based on Kawan and Menezes is correct.

7. ARGUMENT

SUMMARY OF ARGUMENT

Claim Elements not Shown in References - Part I

Claims 21 - 38 are pending. All but four claims (claims 28, 29, 33, and 34) recite

- generating an encryption key K1,
- encrypting that key K1, and
- transmitting the encrypted key K1 to an external destination.

Those recitations have **never been shown** in the references.

The rejection points to some type of encryption found in the references, but that is not encryption of a **key**.

MPEP § 2143.03 states:

To establish prima facie obviousness . . . **all the claim limitations** must be taught or suggested by the prior art.

Therefore, the rejection of these claims cannot stand.

Claim Elements not Shown in References - Part II

Claims 21, 26, 32, 35, 37, and 38 state that an encrypted response-message was received, and that the key K1 (described above) is used to de-encrypt that response-message. Under the claims, the **same** key K1 was also used to encrypt a previous message, which was sent to the sender of the response-message.

That has not been shown in the applied references.

Claim Elements not Shown in References - Part III

"Encrypted Response" not Present

Claim 21 states that

- a key K1 is encrypted,
- the encrypted key is transmitted, and
- an "encrypted response" is received, in response to the transmission.

Neither reference shows an "encrypted response" which is received as a "response" to transmission of an encrypted key, as claimed.

Decryption of "Encrypted Response"
Using Specific Key not Present

Another missing recitation is

- 1) the decryption of the "encrypted response" just discussed, and
- 2) performing that decryption using a specific key.

This two-fold recitation is simply absent from both references.

(This recitation is different from that of Part II, above. In this recitation, an "encrypted response" to something is decrypted. Part II discusses decryption of a generalized message.)

PTO Does not even Assert These Two Recitations
To be Present in References

The Final Action, page 3, lists the claim elements supposedly found in the references. That listing does not assert that the two recitations discussed immediately above are present in the references.

MPEP § 2143.03 states:

To establish prima facie obviousness . . . **all the claim limitations** must be taught or suggested by the prior art.

Claimed use of K1 not Shown in References

Claims 26, 27, 32, and 38 recite de-crypting something using the key K1, which was the key which was previously encrypted and transmitted.

That has not been shown in any reference.

No Valid Teaching Given for Combining References

All rejections are obviousness-type.

The PTO gives a **single rationale** for combining the references in rejecting **all claims**.

In that rationale, the PTO asserts that three motivations lead to a combination of the references, namely,

- 1) pursuit of a "true random bit sequence for

a key,"

2) "to limit available cipher text for cryptanalytic attacks," and

3) attainment of protection of the session key.

However, several problems exist in these rationales.

Problem 1

As to rationale (1), the combined references discuss digital computers.

It is **IMPOSSIBLE** to attain a "true random sequence" using a digital computer.

The following is an excerpt from APPENDIX A, attached hereto.

2.8 RANDOM AND PSEUDO-RANDOM SEQUENCE GENERATION

. . . .

Of course, it is impossible to produce something truly random on a computer.

. . . any random-number generator on a computer . . . is, by definition, periodic.

Anything that is periodic is, by definition, predictable.

And if something is predictable, it can't be random.

A true random-number generator requires some random input; a computer can't provide that.

(Applied Cryptography, page 44, by Bruce Schneier (John Wiley & Sons, New York, 1996, ISBN 0 471 12845 7)).

Thus, it is **impossible** to attain a "true random sequence" using the digital computer of the references. This impossibility is known in the art, as this text testifies.

Therefore, the hypothetical person skilled-in-the-art would never be motivated to combine the references in pursuit of the goal of a "true random sequence." The goal is known to be unattainable.

Further, no expectation of success has been shown, indicating **HOW** the "true random sequence" can actually be attained. MPEP § 706.02(j), attached hereto, requires an expectation of success.

Therefore, motivation (1), attaining a "true random sequence," cannot be used to combine the references.

Problem 2

The second motivation is

2) "to limit available cipher text for cryptanalytic attacks."

This apparently means that the combination reduces the amount of cipher text present, and thus reduces the amount of material available for a hacker to attack.

09/651,979
Art Unit 2137
Docket No. 8490

POINT 1

The desirability of this goal has not been shown in the prior art. MPEP § states 706.02(j):

Contents of a 35 U.S.C. 103 Rejection

. . . the examiner should set forth in the Office action:

. . .

(D) an explanation why one of ordinary skill in the art at the time the invention was made would have been motivated to make the proposed modification.

. . .

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure.

POINT 2

It should be self-evident that one approach to defeating hackers is to **increase** the amount of cipher text in a message. For example, the encrypted message may be buried in a larger message, which larger message is nonsense. (Or the larger message could be unrelated to the encrypted message; the larger message could be a digital photograph, which is a large collection of bytes.)

The concealment of the cipher text in the larger message increases difficulty for a hacker.

Thus, the PTO's goal of limiting availability of cypher text

09/651,979
Art Unit 2137
Docket No. 8490

is not a compelling goal. A cryptographer may pursue the goal of **increasing** cypher text, which is opposite to the PTO's goal.

Therefore, it has been shown so far that (1) the desirability of the PTO's goal has not been shown in the prior art and (2) the PTO's goal is not necessarily desirable in all cases. Consequently, the stated goal does not lead to the combination of references.

POINT 3

The Office Action actually **adds** cipher text to Kawan (eg, the "encrypted response" of claim 21(c), as explained below). That does not "limit" available cipher text, but **increases** available cipher text. Consequently, the combination of references **contradicts** the stated goal.

The stated goal is self-defeating. It teaches **against** the PTO's combination of references.

POINT 4

Motivation (2) is a conclusory statement, unsupported by evidence. The PTO has not provided evidence indicating **how** the combination of references actually imposes the "limit" sought.

If the PTO does not show how the motivation is fulfilled, then, as a matter of logic, the PTO has not shown how the motivation leads to the combination of references.

09/651,979
Art Unit 2137
Docket No. 8490

Also, if no such showing is made, then no expectation of success has been shown either.

Therefore, Appellant submits that motivation (2) is insufficient to combine the references.

Problem 3

The third motivation is

3) attainment of protection of the session key.

POINT 1

This is also a conclusion lacking support. The PTO has not shown **how** the combination of references actually provides any protection.

POINT 2

You can combine certain references and thereby protect a session key, but without attaining claim 21. Thus, the goal of protecting a session key does not necessarily lead to claim 21.

The Office Action must show how its combination of references not only (1) protects a session key, but also (2) attains claim 21.

POINT 3

Numerous claims recite processes unrelated to "protection of a session key." Even assuming those processes to be present in the references, the PTO has not shown how the goal of "protecting the session key" leads to inclusion of those **other** processes in the combination of references. Without those processes, these claims are not attained.

Conclusion as to Teaching

It has just been shown that

- Motivation (1) is impossible,
- Motivation (2) has not been shown in the prior art, is an unsupported conclusion, and also teaches against the PTO's combination of references, and
- Motivation (3) does not lead to claim 21, and is an unsupported conclusion: how the combination of references protects the session key has not been shown.

Therefore, no valid teaching has been given for combining the references.

Restatement of Conclusion

The Final Action has merely set forth three goals. But it has

not shown how the references, even if combined and not considering the claims, achieve those goals.

And it has further not shown how the references, even if combined to produce the claims, achieve those goals.

Thus, the three goals of the Office Action do not suffice as teachings in favor of combining the references under section 103.

Another Restatement

The Final Action has not connected the three goals to the claims, nor to the references.

**At Best, PTO Merely Asserts that
Individual Claim Elements are Found in the References.**

But PTO does not Show How to Assemble Elements into Claims.

The Final Office Action (page 3, bottom - page 4, top) asserts that the Kawan reference shows some elements of the claims, and that the Menezes reference shows the rest.

However, the Final Action fails to explain how the elements of Menezes are combined with Kawan. Thus, no expectation of success has been shown, as required.

Appellant points out that the mere presence of claim elements in the references is insufficient to reject a claim. The elements can be assembled together in innumerable ways. The Final Action has not shown why a particular assembly which supposedly produces

09/651,979
Art Unit 2137
Docket No. 8490

the claims should be chosen, over other assemblies, which do not.

Further, as explained herein (section entitled "Point 3 - PTO is Modifying Kawan," near page 35), the addition of Menezes to Kawan renders Kawan inoperative. That is not allowed.

Further still, as explained herein (section entitled "Point 4 - No Expectation of Success Shown," near page 38), addition of certain elements of Menezes to Kawan serve no purpose. In such a case, it is clear that the references are being combined based on the claims, because no other purpose is attained. That is a combination based on hindsight, which is not allowed.

**Only SINGLE Rationale for Combining References Was Given,
In Rejecting Parent Claims 21 and 33.**

That is Insufficient for Rejection of Remaining Claims

Despite the fact that eighteen claims were rejected, the PTO gives only a **single** rationale for combining the references.

The PTO must show that all claims **as a whole** are obvious. A rationale for combining the references to produce **each** claim must be given.

MPEP § 2141.02 states:

In determining the differences between the prior art and the claims, the question under 35 USC 103 **is not** whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious.

09/651,979
Art Unit 2137
Docket No. 8490

The PTO is apparently assuming that, once references are combined for the purpose of rejecting parent claims, then the PTO is then free to reject dependent claims, without providing further teaching.

Appellant submits that this is a novel proposition of law, contrary to the MPEP section just cited, and requires a citation of authority if this proposition is to be used.

Comment

Not all points made in this Summary are elaborated below. Some are considered self-explanatory.

END SUMMARY OF ARGUMENT

ARGUMENT

RESPONSE TO 103 - REJECTION OF CLAIMS 21 - 38

Claim 21

Point 1 - All Claim Elements not Found in References, Even if Combined

This discussion will first explain, in an "Overview," two claim recitations which are missing from the references, even if combined. This discussion will then explain other claim recitations which are missing.

Overview

Kawan discusses using a PDA to communicate with an ATM.

Menezes is a handbook of encryption, and discusses generalized aspects of encryption.

ONE MISSING RECITATION

One missing recitation is the "encrypted response" of claim 21. The context of that "encrypted response" will be first explained.

Claim 21 recites

- generating a key K1 in a portable computer,
- encrypting K1, to produce K1(encrypted),
- transmitting K1(encrypted) to an external terminal, such as an ATM, and
- receiving an "encrypted response" from the terminal.

Significantly, under the claim, the terminal transmits the "encrypted response" **in "response"** to the receipt of K1(encrypted).

Appellant repeats: the "encrypted response" is not merely an encrypted message.

- It is a "response."
- And it is **a response to K1(encrypted)**, which is an **encrypted key** (not an encrypted

message).

No such "encrypted response" is found in Kawan.

-- Kawan's PDA receives no encrypted message from the terminal, let alone receiving an encrypted "response."

-- Nor is any such message/response received as a "response" to an **encrypted key** previously transmitted by the PDA.

Menezes cannot be used to supply this missing recitation, because it is simply not found in Menezes. Again, Menezes is a generalized handbook. No interplay between an ATM and a PDA has been shown in Menezes. Thus, even if the references are combined, this recitation is not found.

The claimed "encrypted response" is not found in the references, even if combined.

SECOND MISSING RECITATION

Another missing (twofold) recitation is

- 1) the decryption of the "encrypted response" just discussed, and
- 2) performing that decryption using a specific key.

This recitation is found in claim 21, which recites

-- receiving an encrypted message (the

"encrypted response" above) in a portable computer, and
-- decrypting it using a certain key, K1, which was previously generated by the portable computer.

But no such message is received by Kawan's PDA. And no decryption of the (absent) message using key K1, previously generated in the PDA, is shown in Kawan. Both claim recitations are missing.

Appellant points out that an encrypted message is present in Kawan: Kawan's PDA sends an encrypted message **TO** an ATM. That encrypted message contains a PIN and biometric data. But that does not show claim 21, which recites **receiving** an encrypted message in a portable computer.

And it makes no sense for the ATM of Kawan to send the claimed "encrypted response" to Kawan's PDA. One reason is that the encrypted message, which is sent **from** Kawan's PDA **to** the ATM, contains

- (1) a PIN and
- (2) biometric data, such as a scanned fingerprint.

That makes sense: the ATM wants to identify the owner of the PDA. So the PDA sends a PIN and biometric data to the ATM.

But it makes **no sense** for the ATM to send such data to Kawan's PDA.

- ATMs do not have PINs,
- ATMs do not have fingerprints, and
- ATMs do not verify themselves to customers.

CONCLUSION

Therefore, it has just been shown that two claim recitations are missing from the references. That is sufficient to preclude the rejection of claim 21.

End Overview

Resumption of Point 1

Several elements of claim 21 are not found in the Kawan and Menezes references, even if combined, as will now be explained.

Claim 21 recites using a portable computer to

- 1) generate an encryption key K1,
- 2) encrypt K1,
- 3) transmit K1(encrypted) to an external terminal,
- 4) receive an "encrypted response" from the external terminal, and
- 5) de-crypt that response **using the same key K1.**

Kawan does not Generate Keys in PDA
Nor Perform Encryption in PDA

Claim 21 states that, in the portable computer, key K1 is derived from a seed, and then encrypted.

Kawan discusses use of a PDA, Personal Digital Assistant, to communicate with an ATM, Automated Teller Machine. But Kawan does not discuss generation of keys within the PDA, so the claimed derivation of K1 from a seed is not present in Kawan.

Nor does Kawan discuss performing encryption in his PDA. The closest discussion is found in paragraph 31, where he discusses using an encrypted PIN (Personal Identification Number) and encrypted biometric information (eg, a fingerprint). However, he does not discuss **performing** encryption on those two elements **within the PDA**.

And that lack of encryption within the PDA makes sense. The PIN and the biometric information will not change. They are constant. It would waste processing power to repeatedly encrypt those two elements every time a transaction takes place.

Further, why would plain text of the PIN/biometrics be stored within the PDA, for encryption for each transaction? If the PDA were lost, the finder would obtain access to them.

Thus, it is reasonable to assume that Kawan stores those two elements (PIN/biometrics) **in encrypted form**.

Consequently, no encryption occurs in Kawan.

And Kawan produces no keys in his PDA.

Thus, two claim elements are missing from Kawan: (1) generating K1 from a seed, and (2) encrypting K1. MPEP § 2143.03 states:

To establish prima facie obviousness . . . **all the claim limitations** must be taught or suggested by the prior art.

Even if Menezes shows these recitations in the abstract sense, adding Menezes to Kawan does not produce claim 21. Claim 21 states that the two claim elements are performed **within** the "portable computer," which communicates with an external terminal.

As explained herein, even if Menezes shows the two claim elements, adding the two claim elements to Kawan's PDA makes no sense. This shows (1) lack of motivation to do it and (2) lack of the required expectation of success, as explained below.

Further, even if Kawan does encrypt the PIN and biometric data, that does not show claim 21, which recites encryption of a **key**.

Direction of Message in Kawan is OPPOSITE to that Claimed

As stated above, the only encrypted elements of Kawan are (1) the PIN and (2) the biometric information.

But claim 21 states that an encrypted response is received by the "portable computer" and de-crypted therein. That is not shown

09/651,979
Art Unit 2137
Docket No. 8490

in Kawan's PDA (which is the only element in Kawan which could correspond to the claimed portable computer).

Kawan transmits his encrypted matter **FROM** his PDA **TO** the ATM, to verify the authenticity of the PDA. That transmission is in the **opposite direction** to the transmission of the "response" in claim 21.

And, in Kawan, there is no reason to transmit the encrypted matter (PIN/biometrics) in the direction claimed (ie, from the ATM to the portable computer). One reason is that no encrypted matter exists in the ATM, which could be transmitted to the PDA.

That is, the ATM has no PIN or biometric data which could be sent to Kawan's PDA. Nor would that make any sense: ATMs do not have PINS, nor do they have fingerprints.

Therefore, no transmission of an encrypted response in the claimed direction is found in Kawan. And such transmission would be impossible: no data usable in such a transmission is present in Kawan.

The modification of Kawan renders Kawan inoperative.

Claimed "Response" is Absent from Kawan

Claim 21 recites an "encrypted response." The "encrypted response" is produced in response to the transmission of K1(encrypted).

No corresponding "response" is found in Kawan.

Claimed De-Cryption of "Message" is Absent from Kawan

Since, as just explained, no encrypted message/response is received by Kawan's PDA, no de-encryption of that (absent) message can occur. Thus, the de-encryption of claim 21(c) is necessarily absent, as is using key K1 to perform the (absent) de-encryption.

Interim Conclusion

Therefore,

-- Kawan's PDA performs no key generation.

Thus, the claimed generation of K1 from a seed is absent.

-- No encryption is performed by Kawan's PDA.

Thus, the claimed generation of K1(encrypted) is absent.

-- Kawan may transmit encrypted matter **from** his PDA **to** the ATM, but that is in the **wrong direction**, compared to the claim language.

Thus, the claimed receipt of the encrypted message by the portable computer is absent from Kawan.

-- Since Kawan's PDA does not receive an encrypted message, his PDA cannot de-encrypt any

such message.

Thus, the claim language "receiving an encrypted response from the external terminal, and de-crypting the encrypted response using the plain text of K1" as in claim 21(c) is absent from Kawan.

-- Since Kawan's PDA does not generate any key K1, it cannot use that same key K1 to de-crypt the (absent) message received from the ATM.

Thus, use of **a previously generated** K1 to de-crypt the claimed message is absent from Kawan.

-- Claim 21 recites an "encrypted response," which is received as a "response" to transmission of K1(encrypted). No such "response" is found in Kawan.

Thus, the "encrypted response" of claim 21(c) is absent from Kawan.

These six elements of claim 21 are absent from Kawan.

The addition of Menezes does not rectify these absences, since Menezes does not show these elements either. Menezes just discusses generalized aspects of encryption.

Stating this another way, the only possible relevance of

THIS PAGE BLANK (USPTO)

Menezes lies where Kawan discusses encrypted data. But even if Menezes is added to Kawan in that aspect, claim 21 is still not attained, because the missing elements described above are not supplied.

Consequently, these six claim elements are not found in the references, even if combined. MPEP § 2143.03, cited above, precludes the rejection.

Point 2 - Request for Identification

Appellant, in his Request for Reconsideration mailed on July 18, 2005, requested under 37 CFR §§ 1.104(c)(2) and 35 U.S.C. § 132, that the following elements of claim 21 be identified in the references:

- 1) the "seed,"
- 2) the key K1,
- 3) the "encrypted response,"
- 4) the "encrypted response" received by a "portable computer," and
- 5) de-crypting the "encrypted response" using K1.

In answer to this request, the Final Action, page 8, asserts that Menezes shows the seed. However, Menezes only discusses a generalized seed, not the **claimed** seed.

The claimed seed is used to generate a key K1 which is then

09/651,979
Art Unit 2137
Docket No. 8490

encrypted, and transmitted. That has not been shown in the references.

The Final Action also asserts that K1 is the "session key as described above." (See Final Action, page 4, top.) But, again, that "session key" is discussed in Menezes, which discusses a generalized session key. And the claim states that K1 is encrypted. Neither reference shows that.

As to the remaining elements, the Final Action's response provides no identification, but merely asserts that the Final Action has shown the elements in the references. Appellant submits that this Brief contradicts that assertion.

MPEP § 2143.03 states:

To establish prima facie obviousness . . . **all the claim limitations** must be taught or suggested by the prior art.

Point 3 - PTO is Modifying Kawan

The PTO is modifying Kawan. MPEP § 2143.01 prohibits this:

THE PROPOSED MODIFICATION CANNOT RENDER THE
PRIOR ART UNSATISFACTORY FOR ITS INTENDED
PURPOSE.

. . .
THE PROPOSED MODIFICATION CANNOT CHANGE THE
PRINCIPLE OF OPERATION OF A REFERENCE.

. . .

If the proposed modification or combination of
the prior art would change the principle of
operation of the prior art invention being

modified, then the teachings of the references are not sufficient to render the claims prima facie obvious.

That is, the PTO is

- Adding key-generation (K1) to Kawan's PDA, where Kawan has no key-generation.
- Adding encryption of key K1 to Kawan's PDA, where Kawan encrypts no key.
- Adding transmission of the encrypted K1 to Kawan, where Kawan transmits no key.
- Adding transmission of an encrypted message **from** Kawan's ATM **to** the PDA. But that message appears to serve no purpose, and no purpose has been stated.
- Adding de-cryption of that (non-existent) message.
- Using a non-existent key, K1, to de-crypt the non-existent message.

The MPEP section cited above precludes the rejection. Kawan is rendered inoperative, by the addition of several pointless operations supposedly found in Menezes.

- The PTO has not explained exactly what the added key K1 **does** in Kawan.
- The PTO has not explained **why** Kawan

encrypts the key K1.

-- The PTO has not explained how Kawan's ATM decrypts the key K1. (What key does it use ?)

-- The PTO has not explained why Kawan's ATM transmits an "encrypted response" to the receipt of K1.

The PTO's modification of Kawan (1) renders Kawan unfit for its intended purpose and (2) changes the principle of operation of Kawan. And Kawan is rendered inoperative, because somehow his ATM must decrypt K1(encrypted), but the PTO has not explained how that is done. The ATM in Kawan has no key for decrypting K1(encrypted).

Appellant further asserts that these modifications render Kawan inoperative, because, in essence, they are randomly selected processes which are added to Kawan's software, for the purpose of showing Appellant's claims.

No valid reason has been advanced for the addition of these procedures.

No person skilled in the art would randomly add procedures to software, and such random addition will certainly cause the software to crash.

For example, as just explained, the PTO adds to Kawan the transmission of an encrypted message from the ATM to the PDA. How does the software in the PDA now handle this message ? Kawan did not design the software to handle such a message. Unless the

09/651,979
Art Unit 2137
Docket No. 8490

software is re-designed, it will crash. The PTO has shown no re-design, nor a reason for a re-design.

In essence, the PTO proposes adding new sections of code to Kawan's PDA. That will cause Kawan's software to crash. The PTO has not shown how, or why, Kawan's software should be re-designed to handle this new code.

Point 4 - No Expectation of Success Shown

MPEP § 706.02(j) states:

Contents of a 35 U.S.C. 103 Rejection

. . .

To establish a prima facie case of obviousness, three basic criteria must be met.

. . .

Second, there must be a reasonable expectation of success.

. . .

the reasonable expectation of success must . . . be found in the prior art and not based on applicant's disclosure.

As explained above, several claim elements are missing from Kawan. Even if those elements are supplied by Menezes, which is not possible, the PTO must still show an expectation of success. That has not been done. Some examples of lack of expectation of success are illustrated by the following questions.

-- What is the purpose of the claimed
"encrypted response" of claim 21 (which is de-

rypted by K1) if added to Kawan ?

-- Why would the PDA encrypt and deliver key K1 to Kawan's ATM, when the ATM already has an encryption key, which is used to de-encrypt the PIN and the biometrics ?

-- The only encrypted matter present in Kawan, as explained above, contains (1) the PIN and (2) the biometric data. Why would that encrypted matter be transmitted to Kawan's PDA, as a "response" to receipt by an encrypted key K1, received by the ATM ?

-- Why would Kawan transmit the "encrypted response" of claim 21, which would travel **from** Kawan's ATM **to** his PDA ?

Appellant posed these questions in his previous response to the PTO. No answers are given in the Final Action.

Until these, and other, questions have been answered, Appellant submits that no "expectation of success" has been shown, as required by the MPEP.

Since no expectation of success has been shown, the hypothetical person skilled in the art would not attempt the combination of references.

Point 5 - No Teaching for Combining References Given

No valid teaching for combining the references has been given.

The rationale given for combining the references is given in the Final Office Action (mailed 08/23/2005), page 4, second full paragraph. That rationale asserts that three motivations lead to a combination of the references, namely,

- 1) attainment of a true random sequence for a key,
- 2) "to limit available cipher text for cryptanalytic attacks," and
- 3) attainment of protection of the session key.

However, several problems exist in these motivations.

PROBLEM 1

As Menezes states, attainment of a truly random sequence is "a difficult task." (Page 171, section 5.2.) And none of the approaches shown in Menezes, page 172, lead to truly random bit sequences.

APPENDIX A, attached, states that attaining a "truly random sequence" using a digital computer is impossible.

Therefore, the assertion that the combination of references leads to a "truly random sequence" is highly suspect. As a minimum, it is a conclusion unsupported by evidence. Evidence is

required.

PROBLEM 2

Even if a "truly random sequence" is sought, the **combination** of references is not needed to attain it. That is, if the PTO is correct, and Menezes provides "truly random sequences," then Menezes, **by himself**, provides those sequences. There is no reason to add Kawan.

That is, the goal is attained by **ONE** reference alone. The other reference is not needed. The goal does not lead to a combination of references.

PROBLEM 3

The second motivation is "to limit available cipher text for cryptanalytic attacks." Applicant submits that this motivation is self-defeating.

The Office Action actually **adds** cipher text to Kawan (eg, the "encrypted response" of claim 21(c)). That does not "limit" available cipher text, but **increases** available cipher text.

PROBLEM 4

The third motivation is to protect the session key. However, this is a conclusion lacking support. It has not been shown **how** the combination of references actually provides any protection.

Nor has the PTO shown **why** Kawan would need a session key. Kawan discusses a transaction at an ATM, wherein a PDA acts as an intermediary, so that the customer need not punch numbers into the ATM's keypad. In an ordinary ATM transaction, no session key is used. Why is a session key required for Kawan's ATM transaction ? And if it is required, why doesn't Kawan discuss it ?

From another perspective, the Office Action merely asserts that the combined references show claim 21, but without detailed explanation. An explanation is required as to how the motivation of protecting the session key leads to claim 21.

That is, you can combine references in a certain way, and protect a session key, but without attaining claim 21. The Office Action must show how the combination of references not only protects a session key, but also attains claim 21. Nor has the Office Action shown how the combined references protect the session key more effectively.

Point 6 - References Teach Against Claim 21

Sub-Point 6A

Claim 21(a) states that the "records" are stored in "user-accessible memory." Claim 21(b) states that the "seed" for key K1 is generated from the "records."

Thus, any user of the claimed "portable computer" has access

to the "records." That is contrary to Menezes' teachings.

Menezes, in section 5.2, states that "A random bit generator requires a . . . source of randomness." Under claim 21, the "source of randomness" would be the claimed "records." Thus, under claim 21, the "source of randomness" would be "user-accessible."

But Menezes' section 5.2 also states, "The generator must not be subject to observation." That is contrary to storing the "records" in "user-accessible memory," as claimed.

Thus, Menezes teaches against claim 21.

Also, Menezes' section 5.2(ii) lists some events which may be similar to those in the "records" of claim 21. But Menezes states that an "adversary" should be prevented from "observing" those events. (Menezes, section 5.2(ii), fourth sentence.) Again, that is opposite to claim 21, which states that those events are stored in "user-accessible memory."

Menezes teaches against claim 21.

Sub-Point 6B

At least two possibilities exist in Menezes. One is that Menezes

- 1) stores the events in memory then
- 2) later reads the stored events, and
- 3) then applies the read/stored events as inputs to an algorithm, to produce a key.

Another possibility is that Menezes eliminates steps (1) and (2), and applies the events directly to the algorithm, to produce a key.

If the latter possibility occurs, then the recited storage of claim 21(a) is not found in Menezes. In this case, claim 21(a) is not found in the references, even if combined.

Therefore, at least two possible interpretations of Menezes are available. One interpretation does not produce the claim. The PTO must show why the other interpretation is compelling. That has not been done.

**Point 7 - "Records" in "User-Accessible Memory" used for "Seed"
Not Shown in References**

Claim 21 recites a "portable computer," and

- a) storing records of events experienced by the computer in user-accessible memory within the computer.

Claim 21 also recites using some of the "records" as a "seed" for producing a cryptographic key K1.

That has not been shown in the applied references.

Appellant requested that following be identified in the applied references:

- The "records,"
- The "user-accessible memory," and

09/651,979
Art Unit 2137
Docket No. 8490

-- The "seed."

Appellant can find no identification in the Final Action.

Partial Conclusion as to Claim 21

Even if the references are combined, several claim elements are missing.

No valid teaching has been given for combining the references.

Menezes teaches against the concept of deriving a "seed" from data stored in "user-accessible memory."

No expectation of success has been shown. For example, no explanation has been given of what the claimed "encrypted response" would do, if added to Kawan.

Remaining Claims

The preceding discussion applies to the remaining claims. Specifically, the "Interim Conclusion" given above is here repeated, which shows that several elements are absent from the references, even if combined.

Interim Conclusion (Repeated)

-- Kawan's PDA performs no key generation.

Thus, the claimed generation of K1 from a seed is absent.

-- No encryption is performed by Kawan's PDA.

Thus, the claimed generation of K1(encrypted) is absent.

-- Kawan may transmit encrypted matter **from** his PDA **to** the ATM, but that is in the **wrong direction**, compared to the claim language.

Thus, the claimed receipt of the encrypted message by the portable computer is absent from Kawan.

-- Since Kawan's PDA does not receive an encrypted message, his PDA cannot de-crypt any such message.

Thus, the claim language "receiving an encrypted response from the external terminal, and de-crypting the encrypted response using the plain text of K1" as in claim 21(c) is absent from Kawan.

-- Since Kawan's PDA does not generate any key K1, it cannot use that same key K1 to de-crypt the (absent) message received from the ATM.

Thus, use of a **previously generated** K1 to de-crypt the claimed message is absent from Kawan.

-- Claim 21 recites an "encrypted response," which is received as a "response" to transmission of K1(encrypted). No such "response" is found in Kawan.

Thus, the "encrypted response" of claim 21(c) is absent from Kawan.

Menezes cannot be used to supply the missing claim elements, because they are not found in Menezes.

Each of the remaining claim contains one or more of the recitations just enumerated. As just explained, those recitations are not found in the references, even if combined. MPEP § 2143.03 states:

To establish prima facie obviousness . . . **all the claim limitations** must be taught or suggested by the prior art.

The rejection does not comply with this MPEP section.

Claim 22

As stated, the above discussion applies to claim 22. In addition, the following points are here made.

Claim 22 depends from claim 21, and states that a "second session key K2, different from . . . K1," is produced and used in a transaction.

At least two possibilities exist.

One is that K2 is used, as in parent claim 21, to de-crypt the "encrypted response." However, as explained above, no such "encrypted response" is found in the references. Thus, such a K2

is not possible to find in the references.

Another possibility is that K2 is used in a different way, under the language of claim 22, which is here repeated:

- d) . . . produce a second session key K2, different from the first session key K1; and
- e) using K2 in a transaction with an external terminal.

That is, K2 could be merely a key used in a transaction, which is unrelated to the transaction of claim 21.

But no such "transaction" as in paragraph (e) has been shown in the references.

Therefore, to repeat:

- If the "transaction" of paragraph (e) is de-encrypting the "encrypted response" as in claim 21, no "encrypted response" is present in the references.
- If the "transaction" of paragraph (e) is another transaction, such a transaction has not been shown in the references.

Claim 23

The discussion of claim 21 applies to claim 23.

Claim 23 recites using specific data as the seed. The Final Action asserts that Menezes, page 172, teaches using similar data

09/651,979
Art Unit 2137
Docket No. 8490

as a seed.

However, the Final Action has not shown, nor even asserted, that Kawan generates a key. Therefore, the Final Action has not shown what Kawan would do with the seed of Menezes.

No likelihood of success has been shown.

Appellant points to In re Payne, 606 F. 2d 303, 203 USPQ 245 (CCPA 1979):

References relied upon to support a rejection under 35 USC 103 must provide an enabling disclosure, ie, they must place the claimed invention in the possession of the public

An invention is not "possessed" absent some known or obvious way to make it.

Claim 24

The discussion of claim 21 applies to claim 24.

Claim 24 recites generating a key K1, encrypting the key K1, generating another key K2, and encrypting K2.

The PTO has not shown encryption of a **key** in the references.

Moreover, under the claim, the seeds for the keys are obtained from user memory. As explained herein, no teaching has been given for combining the references to attain that.

Appellant points out that Kawan generates no keys, and the PTO has not explained what Kawan would do with the keys which the PTO adds to Kawan from Menezes, even if Menezes discusses generating seeds from user-readable memory etc.

Claim 25

The discussion of claim 21 applies to claim 25.

Claim 25 is considered patentable, based on its parent claim.

Claim 26

The discussion of claim 21 applies to claim 26.

Claim 26 recites decrypting a message EM1 which was received from the external terminal, and using K1 to perform the decrypting.

The PTO has not shown an encrypted message in Kawan, which is sent by Kawan's ATM and received by Kawan's PDA.

Also, K1 is a key previously used to encrypt a **key**. That has not been shown in Kawan, or Menezes.

Claim 27

The discussion of claim 21 applies to claim 27.

Claim 27 recites decrypting a message EM2 which was received from the external terminal, and using K2 to perform the decrypting.

The PTO has not shown an encrypted message in Kawan, which is sent by Kawan's ATM and received by Kawan's PDA.

Also, K2 is a key previously used to encrypt a **key**. That has not been shown in Kawan, or Menezes.

Claim 28

The discussion of claim 21 applies to claim 28.

Claim 28 recites:

28. A method, comprising:

a) maintaining a commercially available Personal Digital Assistant, PDA, which has no secure area for storing an encryption key usable to encrypt outgoing data; and

b) using the PDA for encryption and transmission of a message to an external controller in connection with a financial transaction.

Kawan is Modified

The PTO is modifying Kawan. MPEP § 2143.01, cited above, prohibits this.

The PTO is

-- Adding encryption to Kawan, where Kawan has none.

-- Adding transmission of an encrypted message **from** Kawan's PDA to an ATM. But that message appears to serve no purpose, and no purpose has been stated.

Claimed PDA not Shown in Kawan

The claim states that the PDA lacks a secure area for storing a key. Kawan's PDA, taken by itself, may lack such storage.

09/651,979
Art Unit 2137
Docket No. 8490

However, Kawan states that his PDA is required to be combined with a smart card, in order to perform the ATM transaction. (Paragraph 0029, second sentence.) The smart card contains a secure memory. (Paragraph [0019], second sentence.) Thus, the combination of PDA/smart-card contains secure memory, contrary to the claim.

It could be argued that the PDA, by itself, in Kawan does not contain the secure memory. If so, then claim 28(b) is not present. Claim 28(b) states that the "PDA" engages in a financial transaction. In Kawan, the PDA, by itself, cannot perform the financial transaction.

Therefore, Appellant submits that the PDA/smart-card combination of Kawan must be used to show the PDA of claim 28. That combination contains secure memory, contrary to claim 28(a). And Kawan's PDA alone cannot perform claim 28(b), so the PDA-without-smart-card cannot be used to show that element.

That element of claim 28(b) must be the same element as in claim 28(a).

Claim 29

The discussion of claim 21 applies to claim 29.

Claim 29 recites:

29. Method according to claim 28,
wherein the encryption comprises

- a) deriving a seed from data stored in user-accessible memory; and
- b) deriving a session key from said seed, which session key is used in the financial transaction, and not used thereafter.

No Expectation of Success Shown

The PTO has merely asserted that Menezes shows claim 29(a) and (b). But the PTO has not shown how, or why, Kawan would use 29(a) or (b). The MPEP requires that an expectation of success be shown.

Further, claim 29 recites deriving a "session key." As explained herein, Kawan does not use keys. Thus, there is no purpose for adding the session key to Kawan.

Claim 30

The discussion of claim 21 applies to claim 30.

Claim 30 recites generating a key K1, encrypting K1, and transmitting the encrypted key to an external terminal.

That has not been shown in the references, even if combined.

An encrypted **message** may be implied in the references, but not an encrypted **key**.

Claim 31

The discussion of claim 21 applies to claim 31.

Claim 31 is considered patentable, based on its parent.

Claim 32

The discussion of claim 21 applies to claim 32.

In addition, claim 32 states that an encrypted message is received, and de-crypted using K1. Under the parent claim(s), K1 was encrypted and transmitted to an external terminal.

A key K1 which was both (1) encrypted and transmitted externally and (2) used to decrypt the claimed message has not been shown in the references.

Claim 33

The discussion of claim 21 applies to claim 33.

Claim 33 recites:

33. A portable computer, comprising:

- a) means for storing records of events experienced by the computer in user-accessible memory within the computer;
- b) means for using some of the records as a seed for generating an encryption key; and
- c) means for using the encryption key in a transaction with an external terminal.

As explained above, Kawan does not generate a key. Therefore, claim 33(b) is not found in Kawan.

Menezes may show generation of a key, but the PTO has not shown how, or why, that should be applied to Kawan.

Further, the PTO has not shown that claim 33(a) is found in Kawan. If Menezes is used to show that, then the PTO has not shown how, or why, that should be added to Kawan. Kawan is being modified, contrary to the MPEP.

In addition, no valid teaching for combining the references has been given, and no specific teaching leading to claim 33 has been given.

Claim 33 contains three "means" recitations. Section 112 states:

. . . An element in a claim for a combination may be expressed as a means . . . for performing a specified function without the recital of structure, material, or acts in support thereof,

and

such claim shall be construed to cover the **corresponding structure . . . described in the specification and equivalents thereof.**

The PTO has not shown that the two references show the "corresponding structure . . . described in the specification and equivalents thereof."

For example, the PTO has not shown generation of a key in a portable terminal, and using that key in a transaction with an external terminal.

Claim 34

The discussion of claim 21 applies to claim 34.

Claim 34 is considered patentable, based on its parent.

Claims 35 - 37

Claims 35 - 37 are dependent claims, and contain the phrase "wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to encryption," or similar.

As explained above, Kawan does not perform encryption. Thus, the entry of a PIN, as a prerequisite for the (non-existent) encryption is not found.

No explanation has been given as to why Menezes' encryption should be added to Kawan, to produce the recitations in question.

Claim 38

The discussion of claim 21 applies to claim 38.

Claim 38 recites:

38. A method, comprising:

- a) storing records of events experienced by a portable computer in user-accessible memory within the computer;
- b) using some of the records as a seed for generating a session key K1;
- c) encrypting K1 into K1(encrypted) using a public key;
- d) transmitting K1(encrypted) to an external terminal;

09/651,979
Art Unit 2137
Docket No. 8490

- e) at the external terminal, decrypting K1(encrypted) into K1;
- f) encrypting a message M into M(encrypted) using K1 as key;
- g) transmitting M(encrypted) to the portable computer; and
- h) decrypting M(encrypted) using K1 within the portable computer.

Encrypting the key K1 as in claim 38(c) has not been shown in the references, even if combined.

Transmitting and decrypting K1(encrypted), as in claims 38(d) and (e), have not been shown in the references, even if combined.

"Decrypting M(encrypted) using K1 within the portable computer" as in claim 39(h) has not been shown in the references, even if combined.

ADDITIONAL POINTS

Point 1

The Final Office Action, pages 4 and 5, only asserts that subject matter of certain claims is found in the two references.

That is insufficient. MPEP § 706.02(j) states:

Contents of a 35 U.S.C. 103 Rejection

. . . .

To establish a prima facie case of obviousness, three basic criteria must be met.

First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.

Second, there must be a reasonable expectation of success.

Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure.

Appellant points to the last sentence of this MPEP section, which states that "the teaching . . . to make **THE CLAIMED COMBINATION** . . . must . . . be found in the prior art."

EACH CLAIM is a "claimed combination." Thus, a teaching must be given for each claim.

The mere assertion that the claim elements are found in the references is insufficient.

Point 2

The references are contradictory, regarding a "session key." Menezes, top of page 494, states that a session key is used for a **single** transaction.

Kawan, paragraph 31, states that his encrypted PIN and

09/651,979
Art Unit 2137
Docket No. 8490

biometric data can be used for a single transaction, or **multiple** transactions.

Contradictory references cannot be combined.

Point 3

The Final Action, page 6, asserts that the "combined references teach that all data exchanged between the portable computer and external computer is encrypted."

Appellant submits this assertion to be erroneous. And this assertion is a naked conclusion, unsupported by evidence.

The PTO has the burden of proving its assertion that "all data exchanged" is encrypted. No proof has been given.

Further, Kawan discusses communications between his PDA and ATM which are clearly **NOT** encrypted. For example, at the end of paragraph 0009, he is clearly talking about the ordinary information which a customer enters into an ATM, such as a request for a specific dollar amount of money to be dispensed.

Such requests are not encrypted in an ordinary ATM transaction. Why would they be encrypted when Kawan's PDA is used to relay the data to the ATM, as opposed to the customer's punching the data into the ATM directly, on a keypad ?

In addition, to support its position, the PTO (1) refers to "interchange" of data between the PDA and ATM in Kawan and then (2) finds a definition of "interchange" which is "to give in return for

something received."

However, the PTO has not shown where Kawan uses the term "interchange." Also, the definition found by the PTO does not state that the item given "in return" is encrypted. And the PTO has not shown the context of "interchange" in Kawan. For example, in Kawan, data is given to the ATM, and money is received in return. That can be the "interchange." But no encryption is shown, much less an "encrypted response."

Point 4

The Final Action asserts that, since all data transferred in Kawan is encrypted, an "encrypted response" is present.

However, as just explained, the PTO's premise (that all data transferred is encrypted) is false.

Further, the claims are read **as a whole**. The mere presence of an "encrypted response" is insufficient.

In claim 21, the **claimed encrypted response** is a "response" to receipt of an **encrypted key**. No encrypted key has been shown in Kawan. Therefore, no "response" to an encrypted key can be found in Kawan.

Point 5

The Final Action, page 7, asserts that, in Menezes, the same key is used for encryption and decryption.

However, as explained herein, no valid teaching has been given for combining the references.

Further, even if the PTO's assertion is correct, it is not relevant. The claims state that key K1 is used **both** to (1) encrypt a key and (2) decrypt a response.

Encryption of a **key** has not been shown in the references. Menezes use of a single key for both encryption and decryption does not show encryption of a key.

Point 6

The Final Action, page 7, second paragraph, has been addressed in the Brief. The Brief shows how Kawan is being improperly modified, and rendered inoperative.

Point 7

The Brief has addressed the paragraph of the Final Action which bridges pages 7 and 8.

Point 8

As to the Final Action, page 8, last paragraph - page 9, second full paragraph (ending with "the 'seed' has been described above"), the Brief has demonstrated that Menezes teaches that the seed should be kept secret. That is contrary to the claims.

Further, even if the Final Action is correct in this respect,

the rejections can be fully rebutted on other grounds.

Point 9

As to the third full paragraph of page 9 of the Final Action (relating to claims 22 - 32, 34, and 38), Appellant points out that the claim elements in question have not, in fact, been shown in the prior art. The Brief explains this.

Point 10

As to the fourth full paragraph of page 9 of the Final Action (relating to a PIN in Kawan), Appellant repeats his statement made in his previous response:

Claims 35 - 37 are dependent claims, and contain the phrase "wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to encryption," or similar.

As explained above, Kawan does not perform encryption. Thus, the requirement of a PIN, as a prerequisite for the (non-existent) encryption is not found.

In attempting to rebut Appellant's statement, the Final Action asserts that "Kawan requires a verified PIN before any communication can begin and therefore before any encryption can occur."

However, as explained herein, Kawan's PDA performs no

09/651,979
Art Unit 2137
Docket No. 8490

encryption. And none has been shown in the PTO's rebuttal.

Thus, it cannot be correct to state that Kawan requires a PIN before encryption.

As to the "verified PIN" of the rebuttal, Appellant points out that no encryption process in Kawan, as claimed, has been shown. Therefore, no PIN can be entered "before any encryption," as the PTO asserts.

If the encryption is not present, no time "before" that (nonexistent) encryption can exist.

Re: 112 - Rejections

Claims 21, 33, and 38, and their dependents, were rejected under section 112, because of the word "some."

Point 1

The basis for the rejection is that "some" is a "relative term." (Final Action, page 2, section 5.) However, the MPEP specifically allows relative terms. MPEP § 2173.05(b) states:

Relative Terminology

The fact that claim language, including terms of degree, may not be precise, does not automatically render the claim indefinite under 35 USC 112, second paragraph.

[Citation.]

Acceptability of the claim language depends on

whether one of ordinary skill in the art would understand what is claimed, in light of the specification.

The mere fact that a "relative term" is used is not a basis for rejection.

Point 2

The rejection is self-contradictory. The rejection asserts that the term "some" is indefinite, but then defines the term as "one or more." (Final Action, page 2, bottom.)

That shows that a person skilled-in-the-art has no problem in ascertaining the meaning of "some."

Point 3

The rejection, page 6, top, asserts that the term "makes it unclear as to how many of the records are used if any at all."

Appellant points out that the claim is not required to state "how many" records are used.

The claim is read as a whole. As to claim 21, for example, "records" are recited. The claim 21(b) states that "some of the records" are used to generate a seed.

Plainly, at least one record is used, and possibly all the records are used.

But the claim is not required to say "how many" records are

09/651,979
Art Unit 2137
Docket No. 8490

used.

The claim is entitled to set forth a range.

Point 4

Applicant points to claim 2 in US patent 5,288,949, which states:

2. A carrier for integrated circuits, comprising:

- a) no more than two layers of conductors;
- b) interconnections among the conductors such that

- i) **some** conductors can be used as signal conductors; and

- ii) other conductors can be used as power conductors which shield the signal conductors from each other.

Therefore, the PTO has approved the word "some" on at least one previous occasion. Consequently, Appellant submits that the PTO must explain why now the term "some" is unacceptable.

In Appellant's previous response, he said:

In view of the use of the word "some" in this patent, which was clearly approved by the PTO, Applicant requests a citation of a court decision in support of the rejection.

(Request for Reconsideration, mailed July 18, 2005, page 2.)

09/651,979
Art Unit 2137
Docket No. 8490

No citation of a court decision was made in the Final Action.

The Final Action, page 6, asserts that the patent containing the claim quoted above "has no relation to the present application."

That assertion misses the point.

The point is that the PTO is maintaining inconsistent positions. Both the patent and the present application use the word "some" in a claim. The PTO approved the term in the patent, but objects to the same term in the present application.

The PTO thus assumes the burden of explaining why now the term "some" cannot be used.

Point 5

The rejection is a summary rejection. It is a naked conclusion, based on no evidence.


Appellant submits that the PTO must present a realistic example showing how the term "some" is fatally indefinite under section 112.

09/651,979
Art Unit 2137
Docket No. 8490

CONCLUSION

Appellant requests the Board to overturn all rejections, and pass all claims to issue.

Respectfully submitted,


Gregory A. Welte
Reg. No. 30,434

NCR Corporation
1700 South Patterson Blvd.
WHQ - 4
Dayton, OH 45479
January 23, 2006
(937) 445 - 4956

ATTACHMENTS:

Appealed Claims
APPENDIX A (Excerpt from Schneier text, "Applied
Cryptography")

APPEALED CLAIMS

21. A method of operating a portable computer, comprising:

- a) storing records of events experienced by the computer in user-accessible memory within the computer;
- b) using some of the records as seed for generating plain text of a first session key K1; and then
- c) encrypting K1, transmitting K1(encrypted) to an external terminal, receiving an encrypted response from the external terminal, and de-crypting the encrypted response using the plain text of K1.

22. Method according to claim 21, and further comprising:

- d) repeating processes of paragraphs (a) and (b) to produce a second session key K2, different from the first session key K1; and
- e) using K2 in a transaction with an external terminal.

23. Method according to claim 21, wherein the records used as seed include at least one element selected from the following group:

- 1) recorded button selections,
- 2) recorded pointer movements,
- 3) recorded data entered by a user,
- 4) current date setting, and

5) current time setting.

24. A method, comprising:

a) using a portable computer to

i) generate a first session key K1, based on one or more seeds derived from data contained in user-accessible memory;

ii) encrypt K1 into K1(encrypted), using a public key PK;

iii) transmitting K1(encrypted) to an external terminal in connection with a first transaction;

b) using the portable computer to

i) generate a second session key K2, based on one or more seeds derived from data contained in user-accessible memory;

ii) encrypt K2 into K2(encrypted), using a the public key PK;

iii) transmitting K2(encrypted) to an external terminal in connection with a second transaction.

25. Method according to claim 24, wherein the data from which as the seeds are derived include at least one element selected from

the following group:

- 1) recorded button selections,
- 2) recorded pointer movements,
- 3) recorded data entered by a user,
- 4) current date setting, and
- 5) current time setting.

26. Method according to claim 24, and further comprising:

- c) in connection with the first transaction,
 - i) receiving into the portable computer an encrypted message EM1 from the external terminal, and
 - ii) de-crypting EM1 using K1.

27. Method according to claim 26, and further comprising:

- d) in connection with the second transaction,
 - i) receiving into the portable computer an encrypted message EM2 from the external terminal, and
 - ii) de-crypting EM2 using K2.

28. A method, comprising:

- a) maintaining a commercially available Personal Digital Assistant, PDA, which has no secure area for

storing an encryption key usable to encrypt outgoing data; and

b) using the PDA for encryption and transmission of a message to an external controller in connection with a financial transaction.

29. Method according to claim 28, wherein the encryption comprises

a) deriving a seed from data stored in user-accessible memory; and

b) deriving a session key from said seed, which session key is used in the financial transaction, and not used thereafter.

30. Apparatus, comprising:

a) a portable computer having

i) no secure area for storing an encryption key used to encrypt outgoing data;

ii) system memory, all of which is accessible to a user of the computer; and

iii) data stored in the system memory, which data changes over time;

b) means for

i) utilizing selected changing data in the

system memory as a seed for generating a session key K1;

ii) encrypting K1 into K1(encrypted); and

iii) transmitting K1(encrypted) to an external terminal.

31. Apparatus according to claim 30, wherein the data used as the seed includes at least one element selected from the following group:

- 1) recorded button selections,
- 2) recorded pointer movements,
- 3) recorded data entered by a user,
- 4) current date setting, and
- 5) current time setting.

32. Apparatus according to claim 31, and further comprising:

c) means for

- i) receiving an encrypted message from the external terminal, and
- ii) de-encrypting the encrypted message using K1.

33. A portable computer, comprising:

a) means for storing records of events experienced by

the computer in user-accessible memory within the computer;

b) means for using some of the records as a seed for generating an encryption key; and

c) means for using the encryption key in a transaction with an external terminal.

34. Method according to claim 33, wherein the records used as the seed include at least one element selected from the following group:

- 1) recorded button selections,
- 2) recorded pointer movements,
- 3) recorded data entered by a user,
- 4) current date setting, and
- 5) current time setting.

35. Method according to claim 21, wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete the transaction without the PIN.

36. Method according to claim 24, wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete

the transaction without the PIN.

37. Method according to claim 26, wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to encryption, and will not complete the transaction without the PIN.

38. A method, comprising:

- a) storing records of events experienced by a portable computer in user-accessible memory within the computer;
- b) using some of the records as a seed for generating a session key K1;
- c) encrypting K1 into K1(encrypted) using a public key;
- d) transmitting K1(encrypted) to an external terminal;
- e) at the external terminal, decrypting K1(encrypted) into K1;
- f) encrypting a message M into M(encrypted) using K1 as key;
- g) transmitting M(encrypted) to the portable computer; and
- h) decrypting M(encrypted) using K1 within the portable computer.

BEST AVAILABLE COPY

APPLIED CRYPTOGRAPHY, SECOND EDITION

PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C

BRUCE SCHNEIER



John Wiley & Sons, Inc.

New York • Chichester • Brisbane • Toronto • Singapore

APPENDIX A

name, his public key, and any other important information about the user. This signed compound message is stored in the KDC's database. When Alice gets Bob's key, she verifies the KDC's signature to assure herself of the key's validity.

In the final analysis, this is not making things impossible for Mallory, only more difficult. Alice still has the KDC's public key stored somewhere. Mallory would have to substitute his own public key for that key, corrupt the database, and substitute his own keys for the valid keys (all signed with his private key as if he were the KDC), and then he's in business. But, even paper-based signatures can be forged if Mallory goes to enough trouble. Key exchange will be discussed in minute detail in Section 3.1.

2.8 RANDOM AND PSEUDO-RANDOM-SEQUENCE GENERATION

Why even bother with random-number generation in a book on cryptography? There's already a random-number generator built into most every compiler, a mere function call away. Why not use that? Unfortunately, those random-number generators are almost definitely not secure enough for cryptography, and probably not even very random. Most of them are embarrassingly bad.

Random-number generators are not random because they don't have to be. Most simple applications, like computer games, need so few random numbers that they hardly notice. However, cryptography is extremely sensitive to the properties of random-number generators. Use a poor random-number generator and you start getting weird correlations and strange results [1231,1238]. If you are depending on your random-number generator for security, weird correlations and strange results are the last things you want.

The problem is that a random-number generator doesn't produce a random sequence. It probably doesn't produce anything that looks even remotely like a random sequence. Of course, it is impossible to produce something truly random on a computer. Donald Knuth quotes John von Neumann as saying: "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin" [863]. Computers are deterministic beasts: Stuff goes in one end, completely predictable operations occur inside, and different stuff comes out the other end. Put the same stuff in on two separate occasions and the same stuff comes out both times. Put the same stuff into two identical computers, and the same stuff comes out of both of them. A computer can only be in a finite number of states (a large finite number, but a finite number nonetheless), and the stuff that comes out will always be a deterministic function of the stuff that went in and the computer's current state. That means that any random-number generator on a computer (at least, on a finite-state machine) is, by definition, periodic. Anything that is periodic is, by definition, predictable. And if something is predictable, it can't be random. A true random-number generator requires some random input; a computer can't provide that.

Pseudo-Random Sequences

The best a computer can produce is a pseudo-random-sequence generator. What's that? Many people have taken a stab at defining this formally, but I'll hand-wave here. A pseudo-random sequence is one that looks random. The sequence's period

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.